WHAT IS CLAIMED IS:

1   1.   An apparatus for protecting a first computer system from

2   an intrusion such as a computer virus or an unauthorized access,

3   said apparatus comprising:

4   a second computer system coupled to said first computer

5   system, said second computer system capable of detecting said

6   intrusion before said intrusion reaches said first computer system.

1   2.   The apparatus as set forth in Claim 1 wherein said second

2   computer system is capable of deleting said intrusion after said

3   second computer system detects said intrusion.

1   3.   The apparatus as set forth in Claim 2 wherein said second

2   computer system is capable of deleting said intrusion by erasing

3   data within said second computer system.

1   4.   The apparatus as set forth in Claim 3 wherein said data

2   erased by said second computer system comprises one of: a computer

3   virus software program, an operating system of said second computer

4   system, and at least one computer software program within said

5   second computer system.

1   5.   The apparatus as set forth in Claim 3 wherein after said

2   second computer system has deleted said intrusion by erasing data

3   within said second computer system, said second computer system is

4   capable of receiving a clean version of data that existed in said

5   second computer system before said intrusion occurred.

1   6.   The apparatus as set forth in Claim 5 wherein said second

2   computer system comprises a restoration controller capable of

3   supplying to said second computer system said clean version of said

4   data after said second computer system has deleted said intrusion

5   by erasing data within said second computer system.

1   7.   The apparatus as set forth in Claim 5 wherein said second

2   computer system is capable of receiving said clean version of said

3   data from one of: (1) said first computer system, and (2) an

4   external backup copy of said clean version of said data.

1   8.   The apparatus as set forth in Claim 1 wherein said second

2   computer system comprises a peripheral switch that is capable of

3   switching control of at least one computer peripheral from said

4   second computer system to said first computer system and from said

5   first computer system to said second computer system.

1   9.   The apparatus as set forth in Claim 8 further comprising

2   a hardware control switch coupled to said first computer system,

3   said hardware control switch capable of causing said peripheral

4   switch of said second computer system to switch control of said at

5   least one computer peripheral from said second computer system to

6   said first computer system.

1   10.   The apparatus as set forth in Claim 1 wherein said second

2   computer system comprises:

3   an embedded personal computer;

4   a data transfer switch coupled to said embedded personal

5   computer and to said first computer system, wherein said data

6   transfer switch is capable of transferring data from said first

7   computer system to said embedded personal computer when said data

8   transfer switch is set in read only mode; and

9   wherein said data transfer switch is capable of transferring

10   data from said from said embedded personal computer to said first

11   computer system and from said first computer system to said

12   embedded personal computer when said data transfer switch is set in

13   read and write mode.

1   11.   The apparatus as set forth in Claim 10 wherein said data

2   transfer switch is exclusively controlled by said first computer

3   system.

1   12.   The apparatus as set forth in Claim 1 wherein said second

2   computer system is capable of receiving all external computer

3   communications that are directed to said first computer system.

1   13. A virus trap computer system for protecting a host

2 computer system from an intrusion such as a computer virus or an

3 unauthorized access, said virus trap computer system comprising:

4   an embedded personal computer coupled to said host computer

5 system, said embedded personal computer capable of receiving all

6 external computer communications that are directed to said host

7 computer system, and capable of detecting said intrusion before

8 said intrusion reaches said host computer system.

1   14. The virus trap computer system as set forth in Claim 13

2 wherein said virus trap computer system is capable of deleting said

3 intrusion by erasing data within said virus trap computer system.

1   15. The virus trap computer system as set forth in Claim 14

2 wherein said data erased by said virus trap computer system

3 comprises one of: a computer virus software program, an operating

4 system of said virus trap computer system, and at least one

5 computer software program within said virus trap computer system.

1   16.   The virus trap computer system as set forth in Claim 14

2   wherein after said virus trap computer system has deleted said

3   intrusion by erasing data within said virus trap computer system,

4   said virus trap computer system is capable of receiving a clean

5   version of data that existed in said virus trap computer system

6   before said intrusion occurred.

1   17.   The virus trap computer system as set forth in Claim 16

2   wherein said virus trap computer system comprises a restoration

3   controller capable of supplying to said virus trap computer system

4   said clean version of said data after said virus trap computer

5   system has deleted said intrusion by erasing data within said virus

6   trap computer system.

1   18.   The virus trap computer system as set forth in Claim 16

2   wherein said virus trap computer system is capable of receiving

3   said clean version of said data from one of: (1) said host computer

4   system, and (2) an external backup copy of said clean version of

5   said data.

1   19. The virus trap computer system as set forth in Claim 13

2 wherein said virus trap computer system comprises a peripheral

3 switch that is capable of switching control of at least one

4 computer peripheral from said virus trap computer system to said

5 host computer system and from said host computer system to said

6 virus trap computer system.

1   20. The virus trap computer system as set forth in Claim 19

2 further comprising a hardware control switch coupled to said host

3 computer system, said hardware control switch capable of causing

4 said peripheral switch of said virus trap computer system to switch

5 control of said at least one computer peripheral from said virus

6 trap computer system to said host computer system.

1   21. The virus trap computer system as set forth in Claim 13

2 comprising:

3   a data transfer switch coupled to said embedded personal

4 computer and coupled to said host computer system;

5   wherein said data transfer switch is capable of transferring

6 data from said host computer system to said embedded personal

7 computer when said data transfer switch is set in read only mode;

8 and

9   wherein said data transfer switch is capable of transferring

10 data from said from said embedded personal computer to said host

11 computer system and from said host computer system to said embedded

12 personal computer when said data transfer switch is set in read and

13 write mode.

1   22. The virus trap computer system as set forth in Claim 21

2 wherein said data transfer switch is exclusively controlled by said

3 host computer system.

1   23.   The virus trap computer system as set forth in Claim 13

2   further comprising:

3   a mass storage device coupled to said embedded personal

4   computer;

5   a restoration controller coupled to said embedded personal

6   computer and to said mass storage device, said restoration

7   controller capable of (1) causing all data on said embedded

8   personal computer and said mass storage device to be erased, and

9   (2) after said data has been erased, supplying a clean version of

10   said erased data to said embedded personal computer and to said

11   mass storage device.

1   24.   The virus trap computer system as set forth in Claim 23

2   further comprising:

3   a mass storage integrity controller coupled to said embedded

4   personal computer and to said mass storage device, said mass

5   storage integrity controller capable of detecting an intrusion on

6   said mass storage device, and capable of requesting said embedded

7   personal computer to cause said restoration controller to cause all

8   data on said mass storage device to be erased.

1   25.   The virus trap computer system as set forth in Claim 13

2   further comprising:

3   a password controller coupled to said embedded personal

4   computer and coupled to a network interface, said password

5   controller capable of (1) receiving a computer communication from

6   said network interface, and (2) identifying a password in said

7   computer communication, and (3) in response to receiving a valid

8   password, allowing said computer communication access to said

9   embedded personal computer.

1   26.   The virus trap computer system as set forth in Claim 25

2   wherein said password controller is coupled to said host computer

3   system, and wherein said host computer system, in response to

4   receiving a valid password from said password controller,

5   is capable of allowing said computer communication access to said

6   host computer system through said embedded personal computer and

7   through said data transfer switch.

1   27. A virus trap computer system for protecting a host

2   computer system from an intrusion such as a computer virus or an

3   unauthorized access, said virus trap computer system comprising:

4   an embedded personal computer coupled to said host computer

5   system, said embedded personal computer capable of receiving all

6   external computer communications that are directed to said host

7   computer system, and capable of detecting an intrusion before said

8   intrusion reaches said host computer system;

9   a mass storage device coupled to said embedded personal

10 computer;

11   a restoration controller coupled to said embedded personal

12 computer and coupled to said mass storage device, said restoration

13 controller capable of deleting said intrusion by erasing data

14 within said embedded personal computer and within said mass storage

15 device, said restoration controller capable of supplying a clean

16 version of said erased data to said embedded personal computer and

17 to said mass storage device; and

18   a mass storage integrity controller coupled to said embedded

19 personal computer and to said mass storage device, said mass

20 storage integrity controller capable of detecting an intrusion on

21 said mass storage device.

1   28.   The virus trap computer system as set forth in Claim 27

2   further comprising a password controller coupled to said embedded

3   personal computer and coupled to a network interface, said password

4   controller capable of (1) receiving a computer communication from

5   said network interface, and (2) identifying a password in said

6   computer communication, and (3) in response to receiving a valid

7   password, allowing said computer communication access to one of:

8   said embedded personal computer and said host computer system.

1   29.   The virus trap computer system as set forth in Claim 27

2   wherein said embedded personal computer, said restoration

3   controller, and said mass storage integrity controller are

4   implemented on one integrated circuit chip.

1   30.   The virus trap computer system as set forth in Claim 28

2   wherein said embedded personal computer, said restoration

3   controller, said mass storage integrity controller, and said

4   password controller are implemented on one integrated circuit chip.

1   31. A method for protecting a first computer system from an

2   intrusion such as a computer virus or an unauthorized access, said

3   method comprising the steps of:

4   coupling a second computer system to said first computer

5   system, and

6   detecting said intrusion in said second computer system before

7   said intrusion reaches said first computer system.

1   32. The method as set forth in Claim 31 further comprising

2   the step of:

3   deleting said intrusion by erasing data within said second

4   computer system.

1   33. The method as set forth in Claim 32 wherein said data

2   erased by said second computer system comprises one of: a computer

3   virus software program, an operating system of said second computer

4   system, and at least one computer software program within said

5   second computer system.

1   34.   The method as set forth in Claim 32 further comprising

2 the step of:

3   after said intrusion has been deleted by erasing data within

4 said second computer system, receiving in said second computer

5 system a clean version of data that existed in said second computer

6 system before said intrusion occurred.

1   35.   The method as set forth in Claim 34 wherein said clean

2 version of data is provided by one of: (1) a restoration controller

3 in said second computer system, and (2) said first computer system,

4 and (3) an external backup copy of said clean version of said data.

1   36.   The method as set forth in Claim 31 further comprising

2 the step of:

3   receiving in said second computer system all external computer

4 communications that are directed to said first computer system.

1   37.   A method for protecting a host computer system from an

2   intrusion such as a computer virus or an unauthorized access, said

3   method comprising the steps of:

4   coupling a virus trap computer system to said host computer

5   system, said virus trap computer system comprising an embedded

6   personal computer coupled to said host computer;

7   receiving in said embedded personal computer all external

8   computer communications that are directed to said host computer

9   system; and

10   detecting said intrusion in said embedded personal computer

11   before said intrusion reaches said host computer system.

1   38.   The method as set forth in Claim 37 further comprising

2   the step of:

3   deleting said intrusion by erasing data within said virus trap

4   computer system.

60

1   39. The method as set forth in Claim 38 wherein said data

2   erased by said virus trap computer system comprises one of:

3   a computer virus software program, an operating system of said

4   virus trap computer system, and at least one computer software

5   program within said virus trap computer system.

1   40. The method as set forth in Claim 38 further comprising

2   the step of:

3   after said intrusion has been deleted by erasing data within

4   said virus trap computer system, receiving in said virus trap

5   computer system a clean version of data that existed in said virus

6   trap computer system before said intrusion occurred.

1   41. The method as set forth in Claim 40 wherein said clean

2   version of data is provided by one of: (1) a restoration controller

3   in said virus trap computer system, and (2) said host computer

4   system, and (3) an external backup copy of said clean version of

5   said data.

1   42.   The method as set forth in Claim 37 further comprising

2   the steps of:

3   switching control of at least one computer peripheral from

4   said virus trap computer system to said host computer system and

5   from said host computer system to said virus trap computer system

6   with a peripheral switch in said virus trap computer system; and

7   using a hardware control switch coupled to said host computer

8   system to cause said peripheral switch of said virus trap computer

9   to switch control of said at least one computer peripheral from

10   said virus trap computer system to said host computer system.

1   43. The method as set forth in Claim 37 further comprising

2 the steps of:

3   coupling a data transfer switch to said embedded personal

4 computer and to said host computer system;

5   transferring data from said host computer system to said

6 embedded personal computer when said data transfer switch is set in

7 read only mode;

8   transferring data from said embedded personal computer to said

9 host computer system and from said host computer system to said

10 embedded personal computer when said data transfer switch is in

11 read and write mode; and

12 exclusively controlling said data transfer switch with said

13 host computer system.

1   44. The method as set forth in Claim 37 further comprising

2 the steps of:

3   coupling a mass storage device to said embedded personal

4 computer;

5   coupling a restoration controller to said embedded personal

6 computer and to said mass storage device;

7   in response to a signal from said restoration controller,

8 causing all data on said embedded personal computer and on said

1   mass storage device to be erased; and

2   after said data has been erased, supplying a clean version of

3   said erased data to said embedded personal computer and to said

4   mass storage device.

1   45.   The method as set forth in Claim 44 further comprising

2   the steps of:

3   coupling a mass storage integrity controller to said embedded

4   personal computer and to said mass storage device;

5   detecting an intrusion in said mass storage device with said

6   mass storage integrity controller; and

7   requesting said embedded personal computer to cause said

8   restoration controller to cause all data on said mass storage

9   device to be erased.

1   46.   The method as set forth in Claim 37 further comprising

2   the steps of:

3   coupling a password controller to said embedded personal

4   computer and to a network interface;

5   receiving a computer communication in said password controller

6   from said network interface;

7   identifying a password in said computer communication; and

8   in response to receiving a valid password, allowing said

9   computer communication access to said embedded personal computer.

1   47.   The method as set forth in Claim 46 further comprising

2   the steps of

3   coupling said password controller to said host computer

4   system; and

5   in response to receiving a valid password in said password

6   controller, allowing said computer communication access to said

7   host computer system through said embedded personal computer and

8   through said data transfer switch.